

AZ-104T00A

Module 05:

Intersite Connectivity



Module Overview

- Lesson 01: VNet Peering
- Lesson 02: VPN Gateway Connections
- Lesson 03: ExpressRoute and Virtual WAN
- Lesson 04: Module 05 Lab and Review

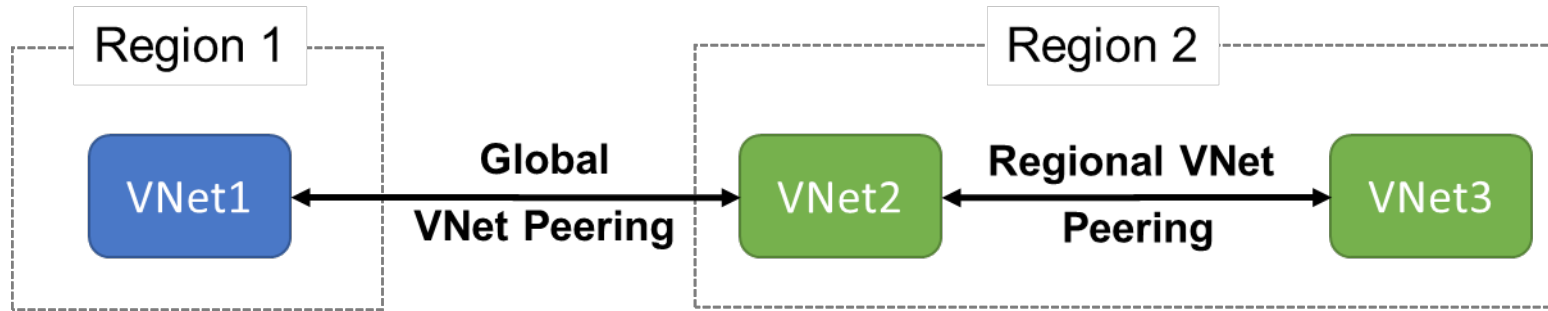
Lesson 01: VNet Peering



VNet Peering Overview

- VNet Peering
- Gateway Transit and Connectivity
- Configure VNet Peering
- Service Chaining
- Demonstration – VNet Peering

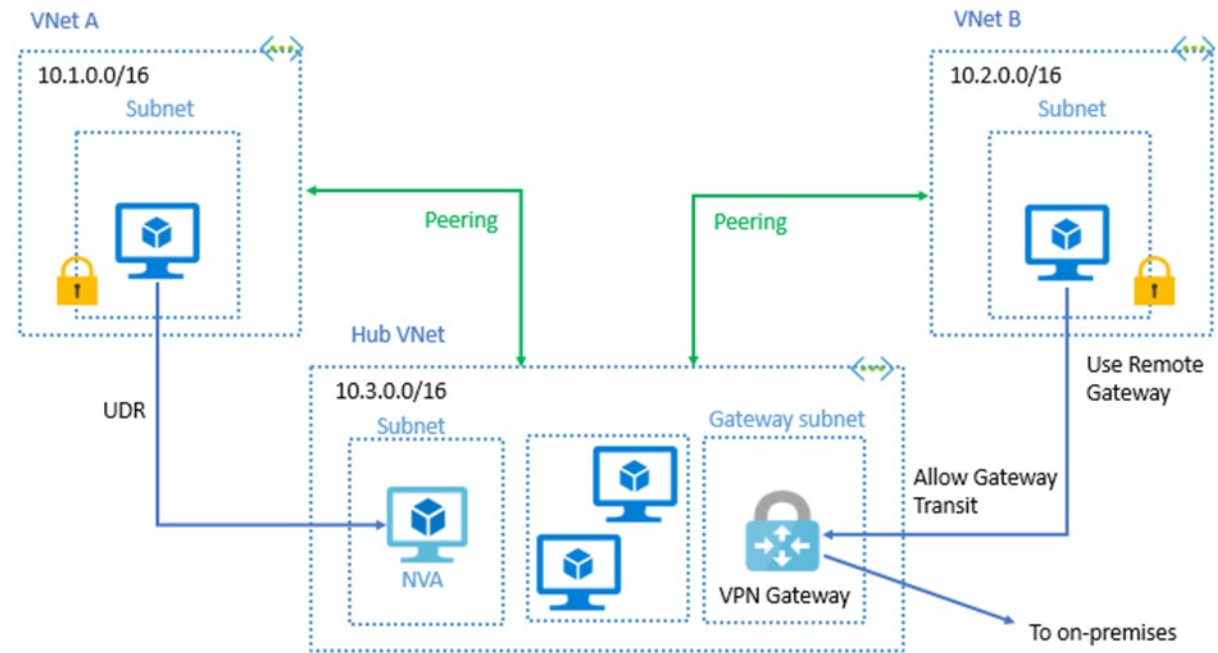
VNet Peering



- VNet peering connects two Azure virtual networks
- Two types of peering: Regional and Global
- Peered networks use the Azure backbone for privacy and isolation
- You can peer across subscriptions
- Easy to setup, seamless data transfer, and great performance

Gateway Transit and Connectivity

- Gateway transit allows peered virtual networks to share the gateway and get access to resources
- No VPN gateway is required in the peered virtual network
- Default VNet peering provides full connectivity



- ✓ IP address spaces of connected networks can't overlap

Configure VNet Peering

- **Allow forwarded traffic** - from within the peer virtual network into your virtual network
- **Allow gateway transit** - Allows the peer virtual network to use your virtual network gateway
- **Use remote gateways** - only one virtual network can have this enabled

Configuration

Configure virtual network access settings

Allow virtual network access from vnet1 to vnet2 ⓘ

Configure forwarded traffic settings

Allow forwarded traffic from vnet2 to vnet1 ⓘ

Configure gateway transit settings

☒ Allow gateway transit ⓘ

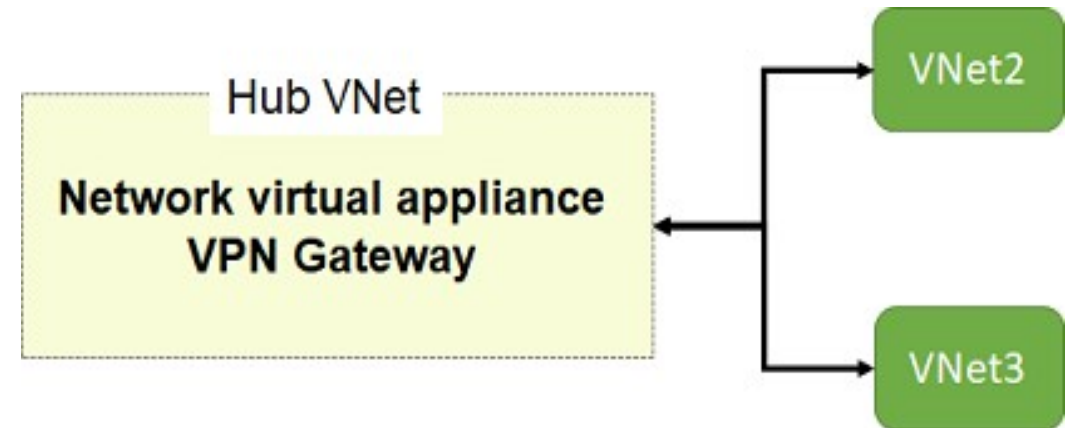
Configure Remote Gateways settings

☐ Use remote gateways ⓘ

✓ If you select 'Allow gateway transit' on one virtual network; then you should select 'Use remote gateways' on the other virtual network.

Service Chaining

- Leverage user-defined routes and service chaining to implement custom routing
- Implement a VNet hub with a network virtual appliance or a VPN gateway
- Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes



Demonstration – VNet Peering

- Configure VNet peering on the first virtual network
- Configure a VPN gateway
- Allow gateway transit
- Confirm VNet peering on the second virtual network

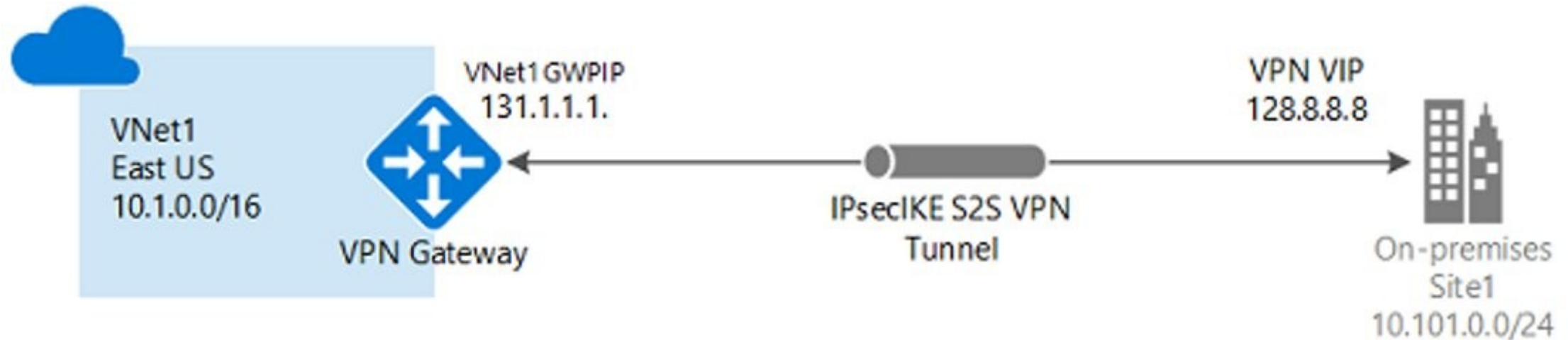
Lesson 02: VPN Gateway Connections



VPN Gateway Connections Overview

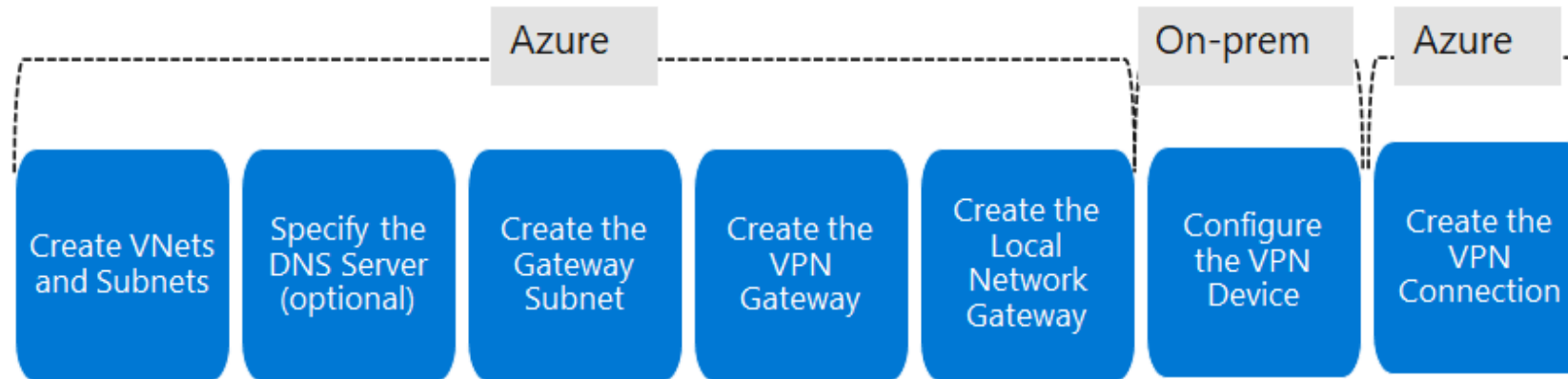
- VPN Gateways
- Implement Site-to-Site VPN Connections
- Create the Gateway Subnet
- VPN Gateway Configuratio
- VPN Gateway SKU and Generation
- Create the Local Network Gateway
- Create the VPN Connection
- High Availability Scenarios
- Demonstration – VPN Gateway

VPN Gateways



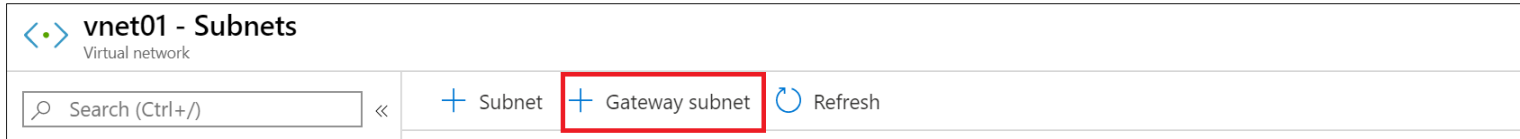
- **Site-to-site connections** connect on-premises datacenters to Azure virtual networks
- **Network-to-network connections** connect Azure virtual networks (custom)
- **Point-to-site (User VPN) connections** connect individual devices to Azure virtual networks

Implement Site-to-Site VPN Connections



- Take time to carefully plan your network configuration
- The on-premises part is necessary only if you are configuring Site-to-Site
- Always verify and test your connections

Create the Gateway Subnet



- The gateway subnet contains the IP addresses; if possible, use a CIDR block of /28 or /27.
- When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings.
- Never deploy other resources (for example, additional VMs) to the gateway subnet.
- Avoid associating a NSG with the gateway subnet.

A screenshot of the 'Add subnet' dialog box in the Azure portal. The dialog has a title bar with 'Add subnet' and a close button (X). Below the title bar, it says 'vnet01'. The form contains several fields: 'Name' with the value 'GatewaySubnet'; 'Address range (CIDR block) *' with a text input containing '10.1.255.0/27' and a green checkmark icon, with a tooltip showing '10.1.255.0 - 10.1.255.31 (27 + 5 Azure reserved addresses)'; 'NAT gateway' with a dropdown menu set to 'None'; an unchecked checkbox for 'Add IPv6 address space'; 'Network security group' with a dropdown menu set to 'None'; 'Route table' with a dropdown menu set to 'None'; 'Service endpoints' with a section header and a 'Services' dropdown menu set to '0 selected'; and 'Subnet delegation' with a section header and a 'Delegate subnet to a service' dropdown menu set to 'None'.

VPN Gateway Configuration

- Most VPN types are Route-based
- Your choice of gateway SKU affects the number of connections you can have and the aggregate throughput benchmark
- Associate a virtual network that includes the gateway subnet
- The gateway needs a public IP address

Create virtual network gateway

Instance details

Name *

Region *

(US) East US

Gateway type * ⓘ

☒ VPN ☐ ExpressRoute

VPN type * ⓘ

☒ Route-based ☐ Policy-based

SKU * ⓘ

VpnGw1

Generation ⓘ

Generation1

VIRTUAL NETWORK

Virtual network * ⓘ

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Enable active-active mode * ⓘ

☐ Enabled ☒ Disabled

Configure BGP ASN * ⓘ

☐ Enabled ☒ Disabled

✓ It can take up to 45 minutes to provision the VPN gateway

Gateway SKU and Generation

Sampling of available SKUs

SKU * ⓘ

VpnGw1

▼

Generation ⓘ

Generation1

▼

Gen	SKU	S2S/VNet-to-VNet Tunnels	P2S IKEv2 Connections	Throughput Benchmark
1	VpnGw1/Az	Max. 30	Max. 250	650 Mbps
1	VpnGw2/Az	Max. 30	Max. 500	1.0 Gbps
2	VpnGw2/Az	Max. 30	Max. 500	1.25 Gbps
1	VpnGw3/Az	Max. 30	Max. 1000	1.25 Gbps
2	VpnGw3/Az	Max. 30	Max. 1000	2.5 Gbps
2	VpnGw4/Az	Max. 30	Max. 5000	5.0 Gbps

- The Gateway SKU affects the connections and the throughput
- Resizing is allowed within the generation
- The Basic SKU (not shown) is legacy and should not be used

Create the Local Network Gateway

- Defines the on-premises network configuration
- Give the site a name by which Azure can refer to it
- The local gateway needs a public IP address
- Specify the IP address prefixes that will be routed through the gateway to the VPN device

Create local network gateway

Name *

VNet1LocalNet ✓

IP address *

33.2.1.5 ✓

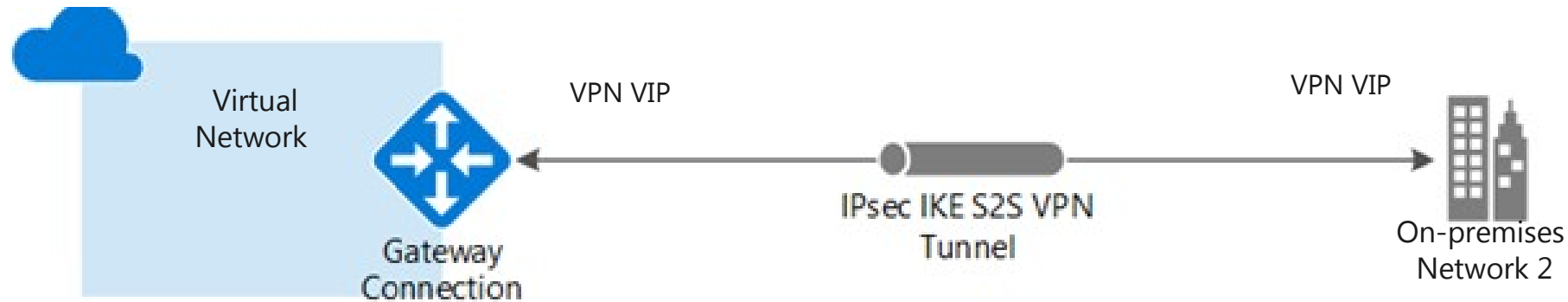
Address space

192.168.3.0/24 ...

Add additional address range ...

☐ Configure BGP settings

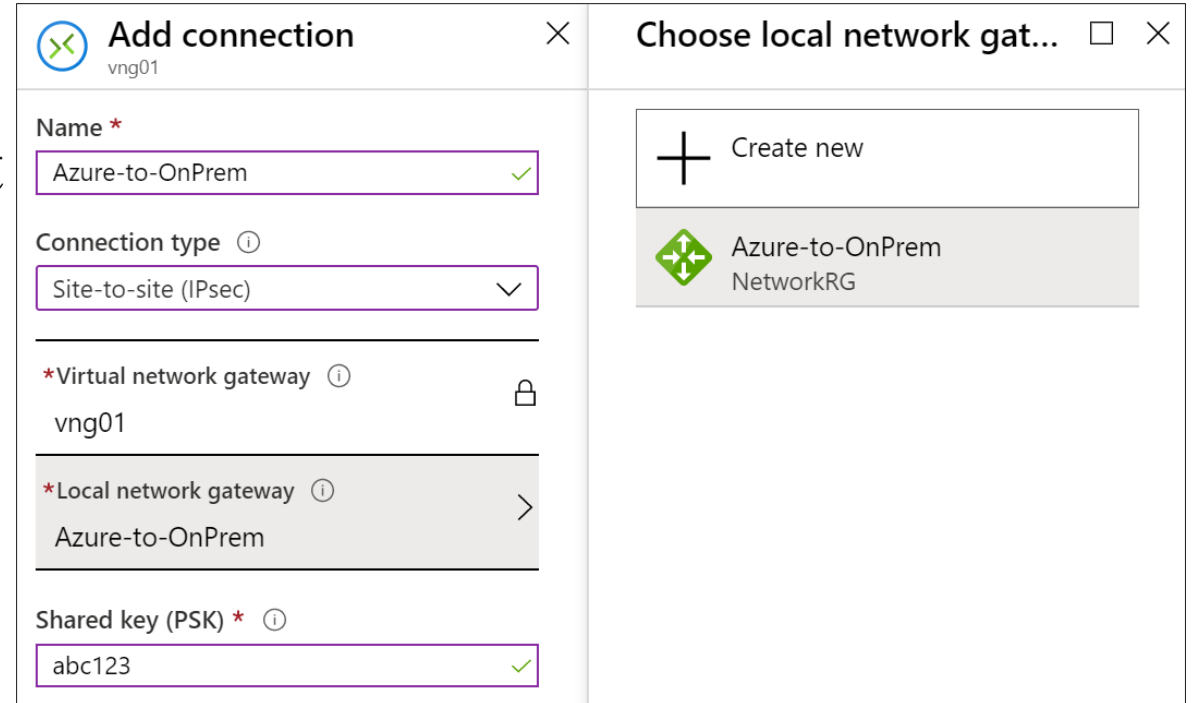
Configure the On-Premises VPN Device



- Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)
- A VPN device configuration script may be available
- Remember the shared key for the Azure connection (next step)
- Specify the public IP address (previous step)

Create the VPN Connection

- Once your VPN gateway is created and the on-premises device is configured, create a connection object
- Configure a name for the connection and specify the type as Site-to-site (IPsec)
- Select the VPN Gateway and the Local Network Gateway
- Enter the Shared key for the connection



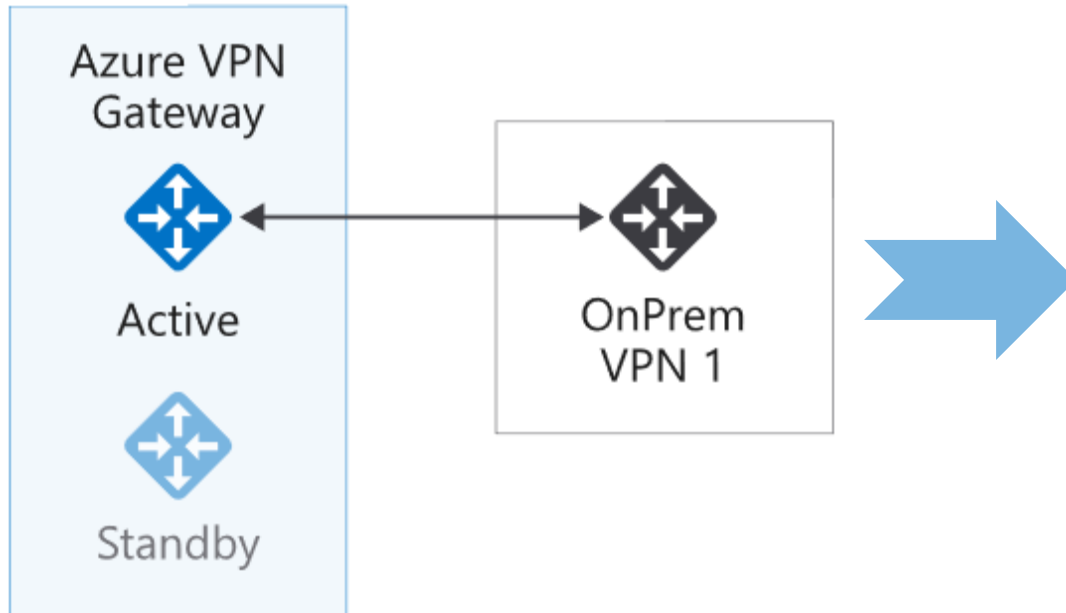
The screenshot shows the 'Add connection' dialog box in the Azure portal. The dialog is titled 'Add connection' with a close button (X) in the top right corner. Below the title bar, the text 'vng01' is displayed. The main form contains the following fields and options:

- Name ***: A text input field containing 'Azure-to-OnPrem' with a green checkmark icon on the right.
- Connection type ⓘ**: A dropdown menu showing 'Site-to-site (IPsec)' with a downward arrow icon.
- *Virtual network gateway ⓘ**: A section with a lock icon on the right, containing a single entry 'vng01'.
- *Local network gateway ⓘ**: A section with a right arrow icon on the right, containing a single entry 'Azure-to-OnPrem'.
- Shared key (PSK) * ⓘ**: A text input field containing 'abc123' with a green checkmark icon on the right.

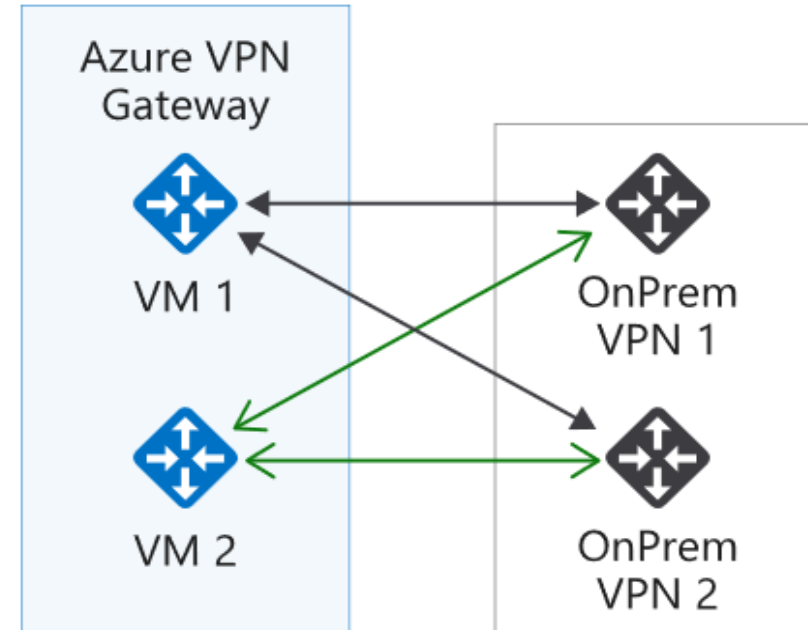
To the right of the main form is a panel titled 'Choose local network gat...' with a close button (X). This panel contains a 'Create new' button with a plus icon and a list of available local network gateways. The first entry is 'Azure-to-OnPrem NetworkRG', which is highlighted with a green diamond icon.

High Availability Scenarios

Active/standby (default)



Active/active



- VPN gateways are deployed as two instances
- Enable **active/active mode** for higher availability

Demonstration – VPN Gateways

- Explore the Gateway subnet blade
- Explore the Connected Devices blade
- Explore adding a virtual network gateway
- Explore adding a connection between the virtual networks

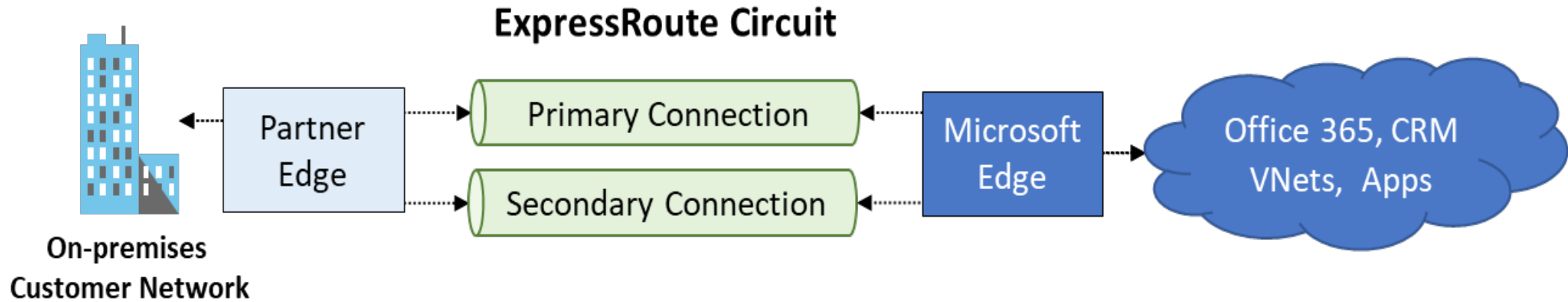
Lesson 03: ExpressRoute and Virtual WAN



ExpressRoute and Virtual WAN Overview

- ExpressRoute
- ExpressRoute Capabilities
- Coexisting Site-to-Site and ExpressRoute
- Virtual WANs

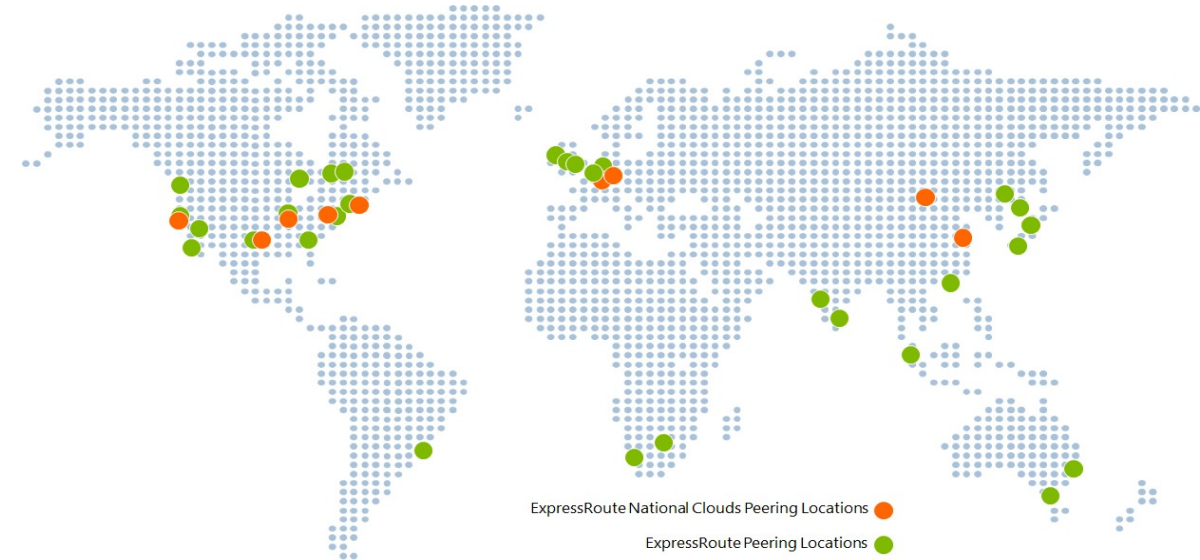
ExpressRoute



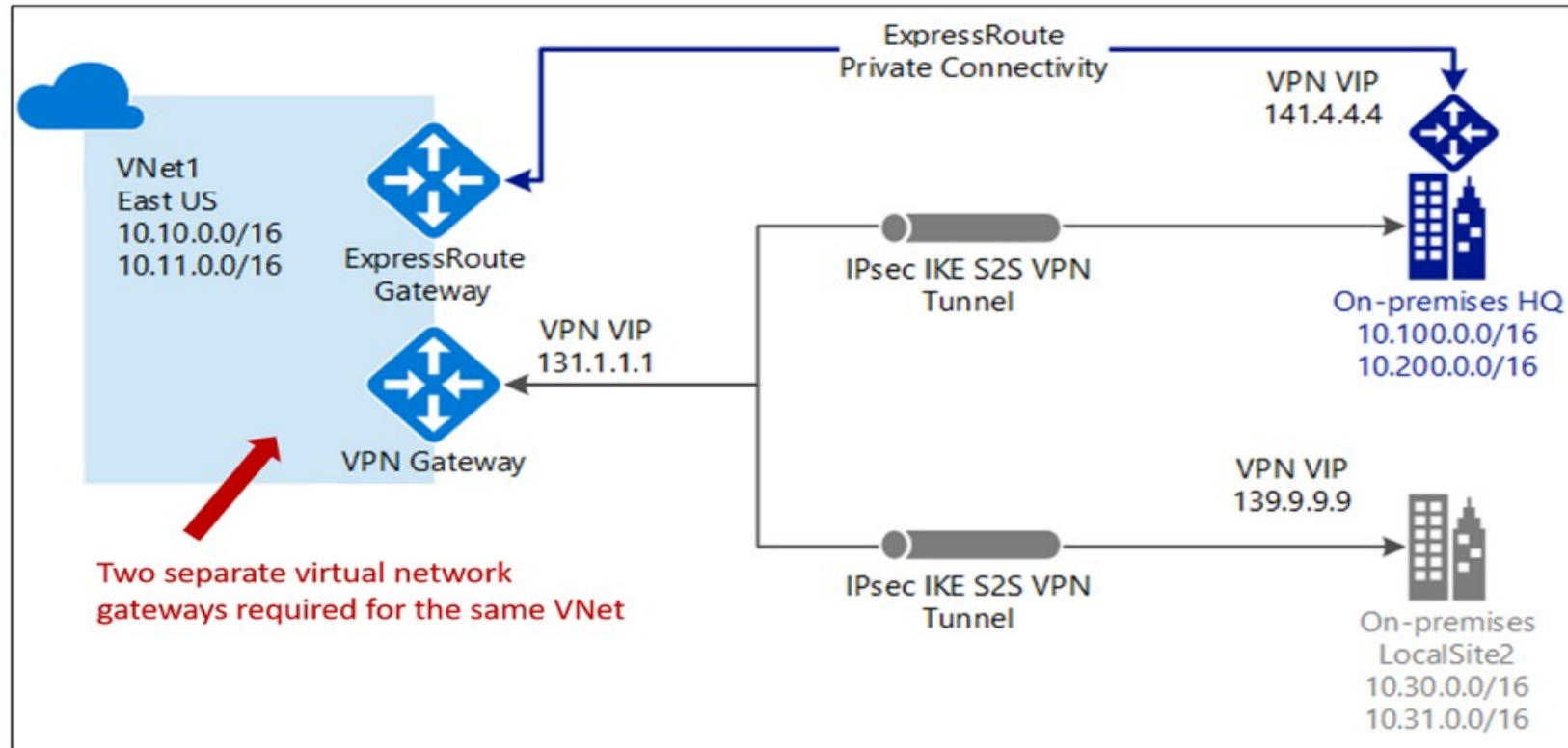
- Private connections between your on-premises network and Microsoft datacenters
- Connections do not go over the public Internet – partner network
- Secure, reliable, low latency, high speed connections

ExpressRoute Capabilities

- Layer 3 connectivity with redundancy
- Connectivity to all regions within a geography
- Global connectivity with ExpressRoute premium add-on
- Across on-premises connectivity with ExpressRoute Global Reach
- Bandwidth options – 50 Mbps to 100 Gbps
- Billing models – unlimited, metered, premium



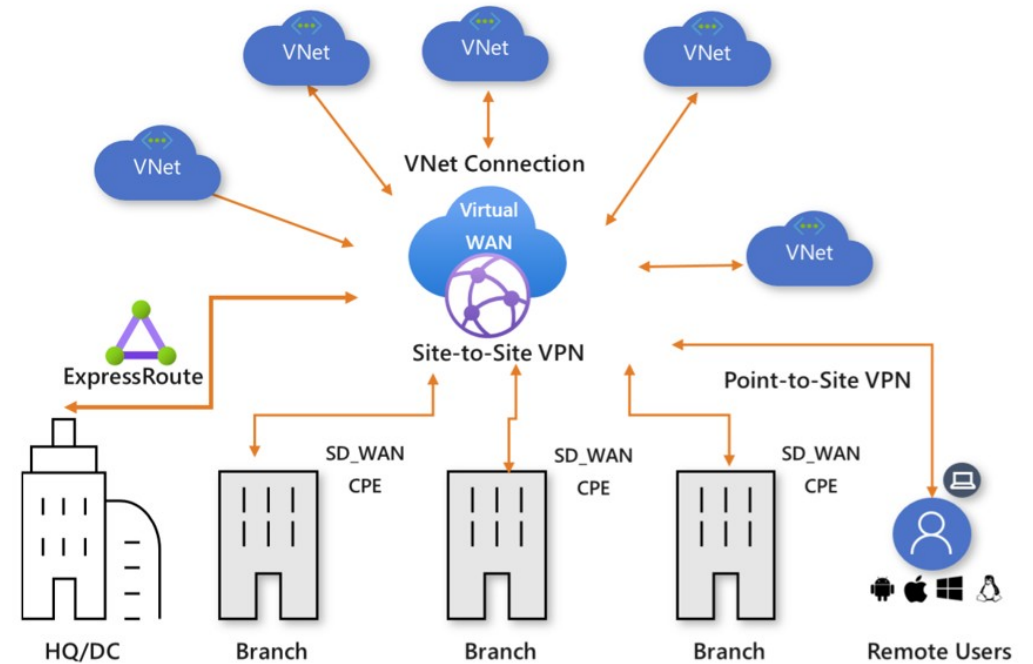
Coexisting Site-to-Site and ExpressRoute



- Use S2S VPN as a secure failover path for ExpressRoute
- Use S2S VPNs to connect to sites that are not connected with ExpressRoute
- Notice two VNet gateways for the same virtual network

Virtual WANs

- Brings together S2S, P2S, and ExpressRoute
- Integrated connectivity using a hub-and-spoke connectivity model
- Connect virtual networks and workloads to the Azure hub automatically
- Visualize the end-to-end flow within Azure
- Two types: Basic and Standard



Lesson 04: Module 05 Lab and Review



Lab 05 - Implement Intersite Connectivity

Lab scenario

Contoso has its datacenters in Boston, New York, and Seattle offices connected via a mesh wide-area network links, with full connectivity between them. You need to implement a lab environment that will reflect the topology of the Contoso's on-premises networks and verify its functionality.

Objectives

Task 1: Provision the lab environment

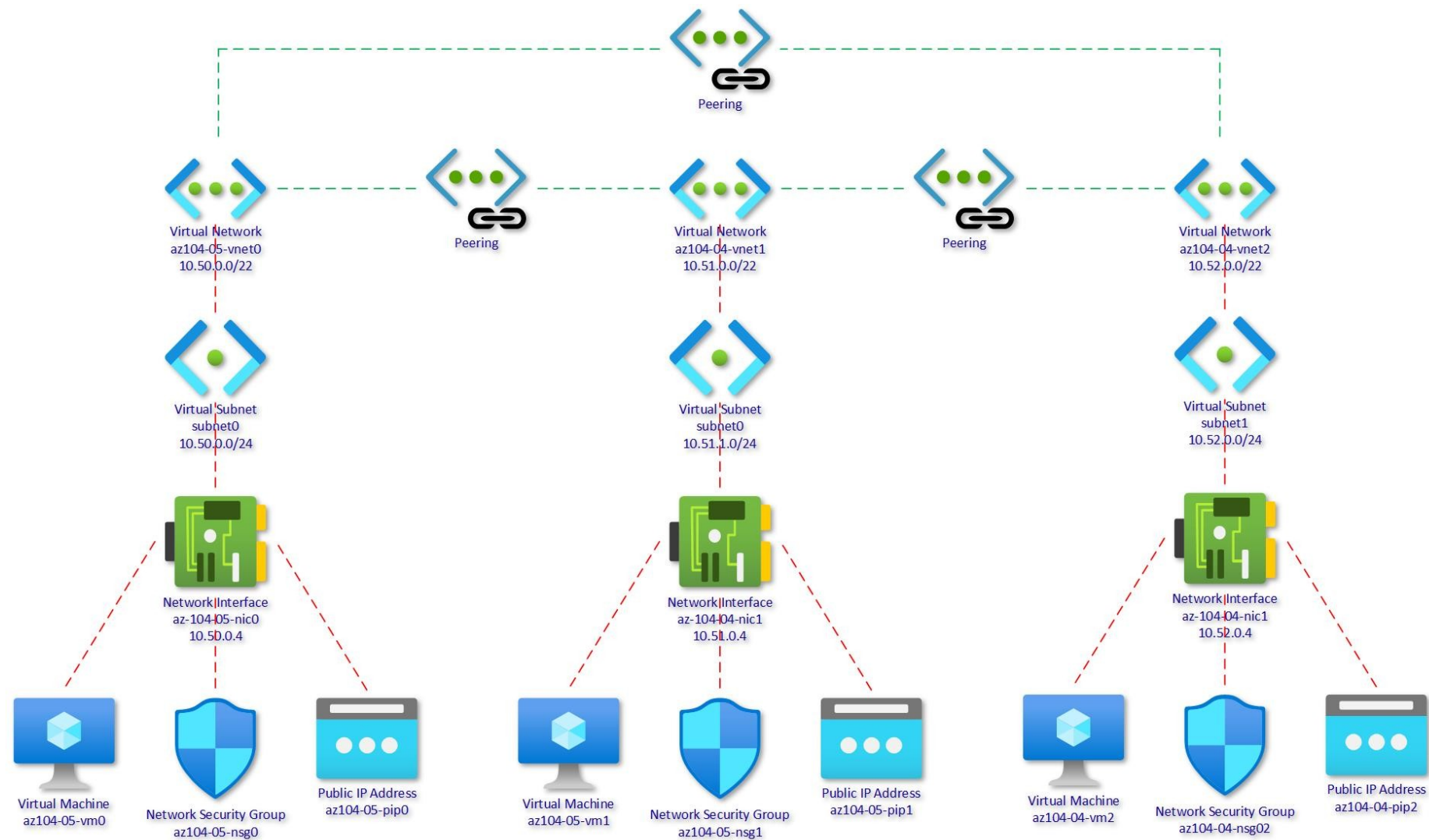
Task 2: Configure local and global virtual network peering

Task 3: Test intersite connectivity

Next slide for
an architecture diagram



Lab 05 – Architecture Diagram



Module Review

- Module Review Questions
- Microsoft Learn Modules (docs.microsoft.com/Learn)
 - Distribute your services across Azure virtual networks and integrate them by using virtual network peering
 - Connect your on-premises network to Azure with VPN Gateway
 - Connect your on-premises network to the Microsoft global network by using ExpressRoute